Netext Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 3, 2012

Rajeev. Koodli
Cisco Systems
Jouni. Korhonen
Nokia Siemens Networks
March 2, 2012

Multi-access Indicator for Mobility
draft-koodli-netext-multiaccess-indicator-03.txt

Abstract

When a Mobile Node attaches to the mobile network using multiple access networks, it is important for the Mobile Network Gateway to know whether the Mobile Node is capable of simultaneous multi-access, so that the former can distribute the traffic flows using the most appropriate interface. This document defines a new EAP attribute which can be used for such an indication to the Mobile Network Gateway. The document also reserves a new MIP6-Feature-Vector flag.

Table of Contents

1. Introduction

With multi-access, a Mobile Node (MN) may be simultaneously attached to a mobile network via multiple access technologies or just be multi-homed. For instance, in the 3GPP architecture [3gpp-4g-2], a MN may be attached to the same Mobile Network Gateway (MNG), called the PGW, via 4G cellular LTE technology as well as the Wireless LAN (WiFi) technology. Such simultaneous access provides opportunity to distribute traffic based on the most appropriate access for the type of traffic in question as well as policy triggers such as the Time Of the Day. In order to accomplish this flow distribution or flow mobility, the MNG needs to know that the MN's attachment is for multi-access (and not handover) purposes and that the MN has the necessary host abstractions to support prefix sharing across access interfaces. This document defines an attribute to be used during the EAP-AKA authentication process so that the 3GPP AAA server understands the MN's capabilities. Subsequently, the 3GPP AAA server provides the MN's capabilities in a Diameter message, enabling the MNG to make the policy decisions to perform flow mobility.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Protocol Overview

In the 3GPP architecture [3gpp-4g-2], two types of "non-3GPP" accesses are supported. In the trusted access model, the access network is considered trustworthy by the 3GPP network operator. An example of a trusted network is another cellular network such as CDMA or WiMAX, but may also include broadband wireline network with WiFi access such as a residential access network operated by the 3GPP cellular service provider. In the untrusted access model, the 3GPP service provider does not possess a trust relationship with the non-3GPP access provider. An example includes WiFi hot spot access.

In the trusted access model, the MN communicates with an Access Network Gateway (ANG). In the untrusted access model, the MN communicates with a secure tunnel (e.g., IPsec) termination node called ePDG. In both the trusted and untrusted access models, the MN performs EAP-AKA [RFC4187] or EAP-AKA' [RFC5448] authentication. In the trusted access model, the EAP-AKA messages are transported from the MN to the ANG over a protocol specific to the access network. In the untrusted access model, the EAP-AKA messages are transported from

the MN to the ePDG over IKEv2 [RFC5996]. Both the ANG and the ePDG communicate with the (3GPP) AAA server using Diameter. This is shown in Figure 1, which we explain further below. The security architecture itself is described in [3gpp-33.402].

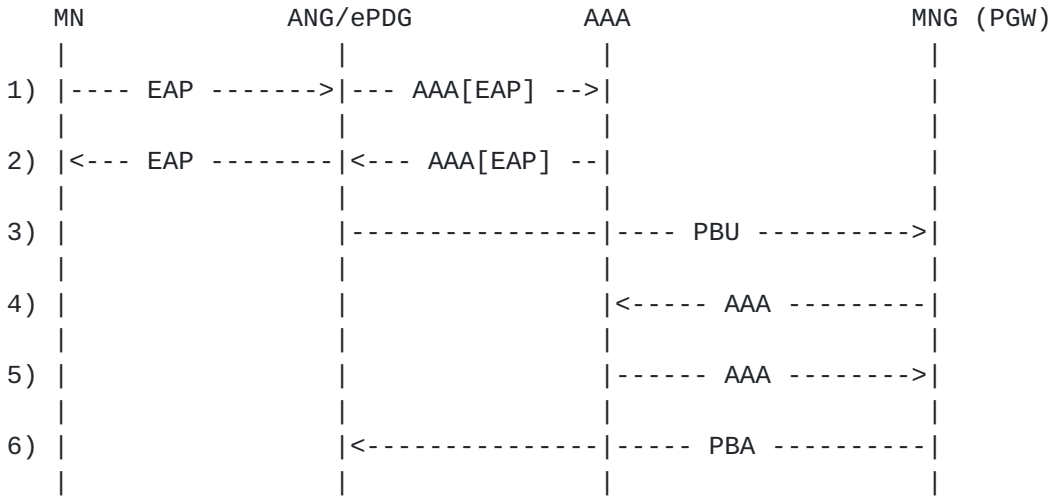

Figure 1: Authentication and Registration

1. The MN attaches to the non-3GPP access network

   The MN performs EAP-AKA or EAP-AKA' authentication. The EAP messages are sent over IKEv2 when the MN is connected using untrusted access.

   As a part of the EAP-AKA procedure, the MN responds with EAP-Response/AKA-Challenge message. In this message, the MN includes a new attribute AT_MA_IND which indicates that the MN's attachment is for multi-access purposes, and that the MN supports the necessary abstraction (Logical Interface) for flow mobility.

   The ANG/ePDG forwards the EAP message to the AAA server using the Diameter EAP application protocol message Diameter EAP Request (DER) message specified in [RFC4072].

2. The 3GPP AAA server verifies through subscription records at the Home Subscriber Server (HSS) that the the MN is allowed to use flow mobility. Subsequently, the AAA server provides the result in a new EAP attribute AT_MA_STATUS in the existing EAP-Request/AKA-Notification message (which is used for indicating the IP Mobility Selection mode [3gpp-24.302]). The EAP message is sent using the Diameter EAP Answer (DEA) message to the ANG/ePDG, which forwards the EAP message to the MN.

3. The ANG/ePDG sends the PMIP6 PBU message.

4. The MNG contacts the AAA server to update the MNG's address for the MN's connection. The MNG includes the MIP6-Feature-Vector AVP with the MN_MULTIACCESS flag set in the AAA request to indicate that multi-access is allowed and supported by the MNG.

5. The AAA server provides the MN's multi-access indication and Logical Interface capability in a MN_MULTIACCESS lag in the MIP6-Feature-Vector AVP [RFC5447].

6. The MNG now understands that the MN is capable of flow mobility. It provides a prefix in the PBA accordingly. For instance, it may provide a new prefix as well as one or more of the already-assigned prefixes in the PBA.

   The ANG/ePDG MUST be able to provide forwarding support for the prefixes provided in the PBA, regardless of the type of attachment indicated in the PBU message.

If the AAA server determines that the UE is not permitted for multi-access flow mobility through the MNG, it does not include the MN_MULTIACCESS flag in the MIP6-Feature-Vector AVP. The absence of the flag is an indication to the MNG that flow mobility is disabled in the subscription. If the AAA server does not understand the AT_MN_IND attribute, it silently discards the attribute, and hence does not send the AT_MA_STATUS attribute back in the EAP-Request/ AKA-Notification message. It also does not provide the MIP6-Feature-Vector to the MNG.

4. Protocol Extensions

Two extensions to existing protocols are defined in this specification. First, a new RFC 5447 MIP6-Feature-Vector AVP capability flag is defined. Second, two new EAP attributes AT_MA_IND and AT_MA_STATUS are defined.

4.1. MN_MULTIACCESS Capability Flag

The MIP6-Feature-Vector AVP [RFC5447] capability flag MN_MULTIACCESS (TBD by IANA) is used by the requesting Diameter node to indicate that it supports multi-access functionality and the feature is also allowed by its policy. The Diameter server uses the flag to authorize the use of multi-access functionality.

The absence of the MN_MULTIACCESS feature flags indicates that either the multi-access feature is not supported/understood or prohibited by

a local policy.

4.2. AT_MA_IND EAP Attribute

The skippable AT_MA_IND EAP attribute is included in EAP-Response/AKA-Challenge message and indicates to the EAP authenticator that the EAP peer (i.e., the mobile node) supports multi-access functionality and this attachment is for multi-access purposes. The attribute is illustrated in Figure 2.

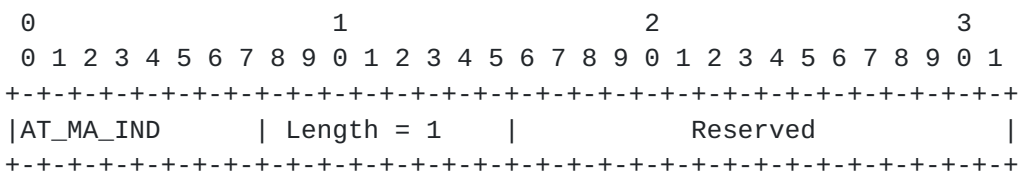

Figure 2: AT_MA_IND EAP Attribute

4.3. AT_MA_STATUS EAP Attribute

The non-skippable AT_MA_STATUS EAP attribute is included in EAP-Request/AKA-Notification or EAP-Request/EAP-Success messages. Due to alignment with [3gpp-24.302] EAP usage this specification only gives examples of cases where EAP-Request/AKA-Notification is used. The attribute indicates to the EAP peer (i.e., the mobile node) that the EAP authenticator supports multi-access functionality and provides the result of the multi-access functionality negotiation. The attribute is illustrated in Figure 3.

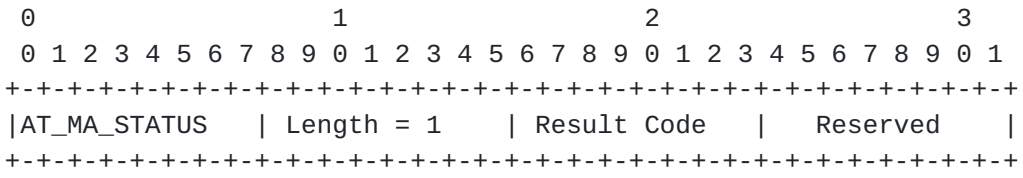

Figure 3: AT_MA_STATUS EAP Attribute

Following Result Codes are defined by this specification:

0 The multi-access functionality was accepted.

128 The multi-access functionality was rejected by a local policy.

5. IANA Considerations

This document defines a new flag (TBD by IANA) for the MIP6-Feature-Vector AVP in RFC 5447, which needs IANA assignment. This document

defines two new EAP attributes: the skippable AT_MA_IND (TBD by IANA) and the non-skippable AT_MA_STATUS (TBD by IANA). Both attributes need IANA assignment.

IANA is also requested to establish a new registry for the AT_MA_STATUS Result Codes. Values between 0-127 are for success codes and values between 128-255 are for error code. The initial values for this registry are listed in Section 4.3. New values for the registry MUST follow the Specification Required [RFC5226].

6. Security Considerations

This documents defines a new EAP attribute to extend the capability of EAP-AKA protocol as specified in Section 8.2 of RFC 4187 [RFC4187]. This attribute is passed from the MN to the AAA server. The document does not specify any new messages or options to the EAP-AKA protocol.

7. Acknowledgement

Thanks to Aeneas-Dodd Noble for flow mobility discussions.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4187] Arkko, J. and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", RFC 4187, January 2006.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC5447] Korhonen, J., Bournelle, J., Tschofenig, H., Perkins, C., and K. Chowdhury, "Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction", RFC 5447, February 2009.

[RFC5448] Arkko, J., Lehtovirta, V., and P. Eronen, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')",

RFC 5448, May 2009.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

8.2. Informative References

[3gpp-24.302] "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP Access Networks, 3GPP TS 24.302 8.7.0, December 2009.", .

[3gpp-33.402] "Security aspects of non-3GPP accesses, 3GPP TS 33.402 8.6.0, December 2009.", .

[3gpp-4g-2] "Architecture Enhancements for non-3GPP accesses, 3GPP TS 23.402 8.7.0, December 2009.", .

[RFC4072] Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", RFC 4072, August 2005.

Authors' Addresses

Rajeev Koodli
Cisco Systems
USA

Email: rkoodli@cisco.com

Jouni Korhonen
Nokia Siemens Networks
Finland

Email: jouni.korhonen@nsn.com